公開日　2022 年 05 月 26 日
改訂日　2022 年 06 月 08 日
株式会社コンテック

SolarView Compact(SV-CPT-MC310)の脆弱性について

■概要

当社製の太陽光発電計測監視装置「SolarView Compact」において複数の脆弱性が存在することが判明しました。本脆弱性を悪意ある攻撃者に悪用された場合、データの盗用や改竄、悪意のあるプログラムを実行しシステムを破壊される等の影響を受ける恐れがあります。
この問題の影響を受ける製品ならびに対策方法・回避策を以下に示しますので、対策または軽減策・回避策の実施をお願いいたします。

■該当製品

製品名　：SolarView Compact
型式　：SV-CPT-MC310、SV-CPT-MC310F
バージョン　：7.21 未満
〈バージョンの確認方法〉
製品に Web ブラウザでアクセスし、メニューから「設定」→「オプション」→「システム更新」を開き、「名称[バージョン]」にて確認できます。

■判明した脆弱性と脆弱性がもたらす脅威

【JVNVU#92327282】

バージョン：7.21 未満で影響を受けるもの

① CVE-2022-29303:「SolarView Compact における OS コマンドインジェクションの脆弱性」
テストメール送信画面から OS が実行できるコマンドを入力することができ、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊、悪意あるプログラムの実行等が行われる可能性があります。

バージョン：6.50 未満で影響を受けるもの

① CVE-2022-29298:「SolarView Compact におけるディレクトリトラバーサルの脆弱性」
ダウンロード画面にて URL が適切に検証されないことにより、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊等を行われる可能性があります。

② CVE-2022-29302:「SolarView Compact における情報漏えいの脆弱性」
Web サーバのコンテンツを編集可能な非公開の画面が存在しており、悪意ある攻撃者に利用されることで情報の盗用・改竄、システムの破壊等を行われる可能性があります。

■対策方法

ソフトウェア(ドライバ)を最新版(Ver.7.21 以降)に更新してください。
最新のソフトウェアは当社 Web サイトより入手できます。
・最新ソフトウェア(SolarView Compact ファームウェア アップデータ)
・SolarViewシリーズ ファームウェア アップデート手順書

■回避策

対策バージョンに更新できないお客様に対し、これらの脆弱性が悪用されるリスクを最小限に抑えるために、当社は以下に示す軽減策を講じることを推奨します。
・本製品をネットワーク回線から切り離す
・本製品のネットワークの上流側にファイアウォールを設置する
・本製品のネットワークアクセスを信頼できる閉域網で構成する
・本製品の「ユーザー設定」にて「ユーザー認証範囲の設定」を「全画面を認証対象にする」で設定する

■お問い合わせ先

ソリューションサポートセンター
TEL:050-3786-4985/03-6625-5541　　E-mail:ssc@jp.contec.com